BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3418571 A1**

(51) Int. Cl. 3: H04L 9/02

(21) Aktenzeichen: P 34 18 571.2
(22) Anmeldetag: 18. 5. 84
(43) Offenlegungstag: 22. 11. 84

DE 3418571 A1

(30) Unionspriorität: (32) (33) (31)
20.05.83 CH 2762-83

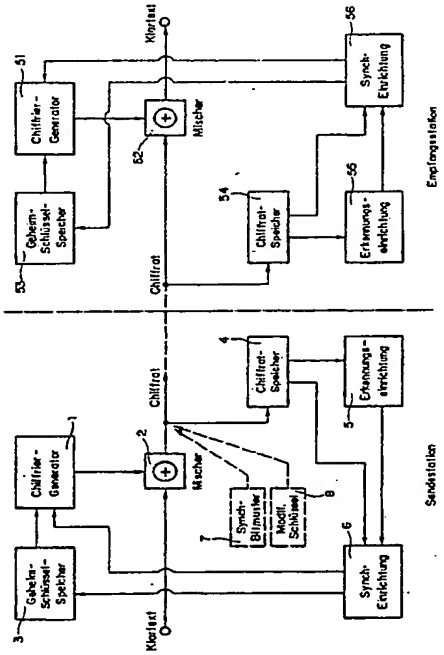
(71) Anmelder:
Gretag AG, Regensdorf, Zürich, CH

(74) Vertreter:
Berg, W., Dipl.-Chem. Dr.rer.nat.; Stapf, O., Dipl.-Ing.; Schwabe, H., Dipl.-Ing.; Sandmair, K., Dipl.-Chem. Dr.jur. Dr.rer.nat., Pat.-Anw., 8000 München

(72) Erfinder:
Klemenz, Hans-Jörg, Dielsdorf, CH; Widmer, Walter Rudolf, Dipl.-El.-Ing., Niederhasli, CH

(54) Verfahren und Vorrichtung zur chiffrierten Datenübermittlung

Sendeseitig wird das Chiffrat durch Mischen des Klartextes mit einer von einem Chiffriergenerator (1) erzeugten Schlüsselimpulsfolge gebildet. Eine Erkennungseinrichtung (5) untersucht in Verbindung mit einem Chiffratspeicher (4) das Chiffrat laufend auf das Auftreten eines bestimmten Synchronisierbitmusters. Sobald dieses auftritt, wird eine Neuinitierung des Chiffriergenerators (1) ausgelöst, wobei als neuer Chiffrierschlüssel oder als Auswahladresse für in einem Schlüsselspeicher (3) vorrätig gehaltene Chiffrierschlüssel eine Anzahl von auf das Synchronisierbitmuster folgenden Chiffratbits verwendet werden. Empfangsseitig wird analog vorgegangen.
Auf diese Weise wird eine Übertragung von zusätzlicher Information bei der Neusynchronisation und damit eine Reduktion des Datendurchsatzes vermieden.



DE 3418571 A1

3418571

Patentansprüche

1. Verfahren zur Uebermittlung von Daten in chiffrierter Form durch sende- und empfangsseitiges Mischen des Klartexts bzw. des Chiffrats mit einer identischen Schlüsselimpulsfolge, die sende- und empfangsseitig in gleichen, durch wenigstens einen Chiffrierschlüssel determinierten Chiffriergeneratoren erzeugt wird, wobei die Chiffriergeneratoren von Zeit zu Zeit unter Wechsel des wenigstens einem Chiffrierschlüssels neu initiiert werden, dadurch gekennzeichnet, dass die Zeitpunkte der Neuinitialisierungen durch das Auftreten eines vorgegebenen Synchronisationsbitmusters im Chiffrat bestimmt werden, und dass der wenigstens eine bei den Neuinitialisierungen neu zu ladende Chiffrierschlüssel aus einer vorgegebenen Anzahl von, vorzugsweise auf das Synchronisationsbitmuster folgenden, Chiffratbits bestimmt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die vorgegebene Anzahl von Chiffratbits direkt als Chiffrierschlüssel verwendet wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die vorgegebene Anzahl von Chiffratbits als Auswahladresse für einen Vorrat von sende- und empfangsseitig in gespeicherter Form vorliegenden Chiffrierschlüsseln verwendet wird.

4. Verfahren nach einem der Ansprüche 1 - 3, dadurch gekennzeichnet, dass bei gegebener Uebertragungsrate das Synchronisationsbitmuster so gewählt wird, dass eine Neuinitialisierung im Mittel alle 0,5 bis 5 sek., vorzugsweise etwa alle Sekunden erfolgt.

5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass das Synchronisationsbitmuster in geheimer, nicht zugänglicher Form gespeichert wird.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass das Synchronisationsbitmuster beim Verbindungsaufbau aktiv übertragen wird.

7. Vorrichtung zur chiffrierten Datenübermittlung mit einer sendeseitigen Chiffrierstation und einer empfangsseitigen Dechiffrierstation, wobei beide Stationen mit einem autonomen Chiffriergenerator und einem Mischer zum Mischen von Klartext bzw. Chiffrat mit einer vom jeweiligen Chiffriergenerator erzeugten Schlüsselimpulsfolge ausgestattet sind und wobei beide Stationen ferner einer Synchronisationseinrichtung aufweisen, mit der wenigstens ein Chiffrierschlüssel in den Chiffriergenerator geladen und dieser dadurch initialisiert werden kann, dadurch gekennzeichnet, dass in Chiffrier- und Dechiffrierstation ein Chiffratspeicher sowie eine an diesen angeschlossene Erkennungseinrichtung vorgesehen sind, welch letztere beim Auftreten eines vorgegebenen Synchronisationsbitmusters im Chiffrat die Synchronisationseinrichtung zu einer Neuinitialisierung veranlasst, und dass die Synchronisationseinrichtung den neu zu ladenden Chiffrierschlüssel aus einer vorgegebene Anzahl von, vorzugsweise auf das Synchronisationsbitmuster folgenden, Chiffratbits bestimmt.

8. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass die Synchronisationseinrichtung die vorgegebene Anzahl von Chiffratbits direkt als Chiffrierschlüssel in den jeweiligen Chiffriergenerator lädt.

9. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass in Chiffrier- und Dechiffrierstation ein Vorrat von Chiffrierschlüsseln gespeichert ist, und dass die Synchronisationseinrichtung den in den Chiffriergenerator neu zu ladenden Chiffrierschlüssel anhand der vorgegebenen Anzahl von Chiffratbits auswählt und lädt.

10. Vorrichtung nach einem der Ansprüche 7-9, dadurch gekennzeichnet, dass Schaltmittel vorgesehen sind, welche das Synchronisationsbitmuster beim Verbindungsaufbau aktiv übertragen.

FO 7.7 KL/rz*/rn*/eh*

PATENTANWÄLTE
MAUERKIRCHERSTRASSE 45 · 8000 MÜNCHEN 80

Anwaltsakte 33 409 18. Mai 1984

*

GRETAG Aktiengesellschaft
Althardstrasse 70
CH-8105 Regensdorf/SCHWEIZ

*

VERFAHREN UND VORRICHTUNG ZUR CHIFFRIERTEN DATENÜBERMITTLUNG

Priorität:

Land:	SCHWEIZ
Aktenzeichen:	2762/83-9
Anmeldetag:	20. MAI 1983

*

eg

☎ (089) 98 82 72 - 74
Telegramme (cable):
BERGSTAPFPATENT München

Telex: 5 24 560 BERG d
Telekopierer. (089) 98 30 49
Kalle Infotec 6350 Gr II + III

Bankkonten: Bayer. Vereinsbank München 453 100 (BLZ 700 202 70)
Hypo-Bank München 4410122 850 (BLZ 700 200 11) Swift Code: HYPO DE MM
Postscheck München 653 43-808 (BLZ 700 100 80)

9-14436/GTN 489/-

Verfahren und Vorrichtung zur chiffrierten Datenübermittlung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur chiffrierten Datenübermittlung gemäss Oberbegriff des Patentanspruchs 1 bzw. 4.

Chiffrier/Dechiffriersysteme dieser Art sind heute allgemein bekannt und verbreitet. Einige typische Vertreter sind zum Beispiel in der US-PS 4 369 434 erwähnt und beschrieben.

Die Neuinitialisierung der Chiffriergeneratoren erfolgt bei diesen bekannten Systemen derart, dass entweder der neu zu ladende Chiffrierschlüssel selber (zufallsmässig erzeugter Zusatz- oder Modifizierschlüssel) und/oder - bei Systemen mit gespeichtem Schlüsselvorrat - eine Auswahladresse für den neu zu ladenden Schlüssel von der die Neuinitialisierung verlangenden Station zur Partnerstation übertragen wird. Durch diese Uebertragung von zusätzlicher Information wird der (Nutz)- Datendurchsatz herabgesetzt, was insbesondere dann ins Gewicht fällt, wenn häufigere Nachsynchronisierungen (z.B. für Späteintritt oder nach Fehlern, häufiger Schlüsselwechsel) nötig oder erwünscht sind.

Durch die Erfindung soll nun dieses Problem überwunden und insbesondere das Verfahren und die Vorrichtung der zur Rede stehenden Art dahingehend verbessert werden, dass zur Neuinitialisierung der Chiffriergeneratoren keine Uebertragung von zusätzlicher Information notwendig ist und damit der Nutzdatendurchsatz dabei nicht reduziert wird.

Das erfindungsgemässe Verfahren und die entsprechende Vorrichtung, welche diesen Anforderungen genügen, sind in den Patentansprüchen 1 und 4 beschrieben. Bevorzugte Ausführungsformen und Weiterbildungen ergeben sich aus den abhängigen Ansprüchen.

Ein ähnliches System ist in der DE-B-1 076 733 beschrieben. Bei diesem bekannten System wird aber beim Auftreten einer bestimmten Datensequenz keine komplette Neuinitialisierung inklusive Schlüsselwechsel vorgenommen, sondern es werden lediglich die Chiffriergeneratoren auf eine definierte, jedesmal gleiche Anfangsstellung rückgesetzt.

Weitere Literaturstellen zum technologischen Hintergrund sind EP-A 0 027 423 und EP-A-0 063 352.

Im folgenden wird die Erfindung anhand der Zeichnung näher erläutert. Die einzige Zeichnungsfigur zeigt ein auf das Wesentlichste reduziertes Blockschema eines Ausführungsbeispiels einer erfindungsgemässen Chiffrier/Dechiffriervorrichtung.

Die dargestellte Chiffrier/Dechiffriervorrichtung entspricht im wesentlichen den in der schon genannten US-PS 4 369 434 angeführten Vorrichtungen. In der Zeichnung sind daher nur die für das Verständnis der Erfindung unmittelbar notwendigen Funktionsblöcke gezeigt. Es sind dies auf Sende- und Empfangsseite je ein Chiffriergenerator 1 bzw. 51, ein Modulo-2-Mischer 2 bzw. 52, ein Schlüsselspeicher 3 bzw. 53, ein Chiffratspeicher 4 bzw. 54, eine Erkennungseinrichtung 5 bzw. 55 und eine Synchronisiereinrichtung 6 bzw. 56.

Mit Ausnahme des Chiffratspeichers 4 bzw. 54 und der Erkennungseinrichtung 5 bzw. 55 stimmt die gesamte Vorrichtung in Aufbau und Funktionsweise mit dem Stand der Technik, wie er z.B. durch die US-PS 4 369 434 repräsentiert ist, überein: Der Chiffriergenerator 1 bzw. 51, der bei jeder Neuinitialisierung via Synchronisiereinrichtung 6 bzw. 56 mit einem neuen Chiffrierschlüssel geladen wird, erzeugt eine Schlüsselimpulsfolge, die im Mischer 2 bzw. 52 zum Klartext bzw. Chiffrat hinzugemischt wird, um das Chiffrat bzw. wieder den ursprünglichen Klartext zu ergeben.

Der Chiffrierschlüssel besteht in der Regel aus mehreren Teil-Schlüsseln, von denen einer ein sogenannter Grund- oder Geheimschlüssel und ein anderer ein sogenannter Zusatz- oder Modifizierschlüssel ist. Letzterer wird üblicherweise bei jeder Neuinitialisierung neu zufallsmässig erzeugt. Der Grund- oder Geheimschlüssel wird im Unterschied dazu nicht jedesmal neu erzeugt, sondern es ist im Schlüsselspeicher 3 bzw. 53 ein grösserer Vorrat an Geheimschlüsseln gespeichert vorhanden, aus denen beim Schlüsselwechsel mittels einer meist zufälligen Auswahladresse jeweils einer ausgewählt und in den Chiffriergenerator geladen wird.

Bei den in der US-PS 4 369 434 detaillierter erläuterten Chiffrier/Dechiffriersystemen werden der zufallsmässige Modifizierschlüssel und die ebenfalls zufällige Auswahladresse für den Geheimschlüssel bei jeder Neuinitialisierung zur Partnerstation übertragen, was zu der schon eingangs erwähnten Datendurchsatzreduktion führt. Beim System gemäss der Erfindung wird anders vorgegangen: Hier wird das Chiffrat sende- und empfangsseitig laufend über eine gewisse Anzahl von Bits auf das Auftreten eines vorgegebenen Bitmusters - des sogenannten Synchronisationsbitmusters - überwacht. Wenn dieses Bitmuster auftritt, wird eine Neuinitialisierung des Chiffriergenerators veranlasst, wobei eine bestimmte Anzahl von auf das Synchronisationsbitmuster folgenden Bits des Chiffrats entweder als neuer Modifizierungsschlüssel oder als Auswahladresse für den neu zu ladenden Geheimschlüssel verwendet werden. Gewünschtenfalls können beide Möglichkeiten auch kombiniert werden, wobei dann z.B. ein Teil dieser nachfolgenden Chiffratbits den neuen Modifizierschlüssel und ein anderer Teil die Auswahladresse für den neuen Geheimschlüssel bilden. Selbstverständlich können auch dem Synchronisationsbitmuster vorausgegangene Chiffratbits als Schlüssel bzw. Auswahladressen benutzt werden.

Zur Realisierung dieser erfindungsgemässen Verfahrensprinzips sind nur wenige zusätzliche Funktionsstufen notwendig, und zwar der Chiffratspeicher 4 bzw. 54 und die Erkennungseinrichtung 5 bzw. 55. Der Chiffratspeicher kann z.B. ein Schieberegister sein, durch welches die Chiffratbits im Takte der Uebertragungsgeschwindigkeit

durchgeschoben werden. Die Erkennungseinrichtung vergleicht die Inhalte einer gegebenen Anzahl von Speicherzellen des Chiffratspeichers mit einem vorprogrammierten Synchronisierbitmuster und löst bei Uebereinstimmung die Neuinitiierung via Synchronisiereinrichtung aus.

Das Synchronisierbitmuster ist vorzugsweise analog wie die Geheimschlüssel geheim, d.h. in nicht zugänglicher Form gespeichert. Es kann dadurch weniger leicht erkannt und gezielt gestört werden.

Bei den heutigen modernen Chiffrier/Dechiffriergeräten sind die meisten Funktionen mittels eines Micro- oder Minicomputers und entsprechender Software implementiert. Dasselbe kann natürlich auch für die einzelnen Funktionsstufen der Vorrichtung gemäss der vorliegenden Erindung gelten.

Durch das erfindungsgemässe Verfahrensprinzip wird also eine Uebertragung von Chiffrierschlüsseln bzw. ihrer Auswahladressen überflüssig. Auf diese Weise kann - im Interesse der kryptologischen Sicherheit - ein sehr häufiger Schlüsselwechsel durchgeführt werden, ohne dass dadurch der Datendurchsatz beeinträchtigt würde. Dasselbe gilt für Nachsynchronisation zum Zweck des Späteintritts oder Synchronisation nach Fehlern etc.

Die Länge des Synchronisierbitmusters ist an sich beliebig. Sie wird mit Vorzug so gewählt, dass bei gegebener Uebertragungsrate im statistischen Mittel eine gewünschte Anzahl - beispielsweise etwa 0,2 bis 2, vorzugsweise rund 1, von Schlüsselwechseln pro Sekunde stattfindet. Bei einer Uebertragungsrate von 19,2 KB/S findet z.B. bei einer Synchronisierbitmusterlänge von 14 Bit etwa alle Sekunden und bei einer Länge von 16 Bit etwa alle 3 Sekunden eine Neusynchronisierung statt.

Die Anzahl der als Chiffrierschlüssel bzw. Auswahladresse benutzten auf das Synchronisierbitmuster folgenden Chiffratbits hängt von den verwendeten Chiffrierschlüsseln selbst bzw. der Anzahl der gespeicherten Schlüssel ab.

Zur Beschleunigung des Verbindungsaufbaus zwischen den Partnerstationen kann für die erste Synchronisation das Synchronisierbitmuster auch aktiv übertragen werden, anstatt zu warten, bis es zufällig erzeugt wird. In der Zeichnung ist dies durch die zwei dargestellten Funktionsblöcke 7 und 8 in der Sendestation angedeutet.Block 7 legt bei der Verbindungsaufnahme das Synchronisierbitmuster auf die Chiffratleitung, Block 8 lässt darauf eine als Modifizierungsschlüssel bestimmte Zufallsbitsequenz folgen. Chiffratspeicher und Erkennungseinrichtung funktionieren in gleicher Weise wie bisher beschrieben.

– Leerseite –

Nummer: 34 18 571
Int. Cl.³: H 04 L 9/02
Anmeldetag: 18. Mai 1984
Offenlegungstag: 22. November 1984